DAWSON COLLEGE

No. IST-04

Title: Accounts Policy

CLASSIFICATION: INFORMATION SYSTEMS & TECHNOLOGY
FIRST ADOPTED: 12 May 2016
AMENDED:

1. Scope

This policy applies to employees with privileged access to accounts, systems, or information within systems, as well those who implement, deploy or manage systems.

2. Definitions

i. *Generic account.* An account that is not tied to a specific person via an employee number or email address. Note that the username itself does not suffice to identify a person. For example, *jsmith* with no other information is generic, but jsmith along with employee number 12345, or external email jsmith@yahoo.com is not generic.
ii. *Shared account*. An account designed to be shared amongst users. By definition this is also a generic account.
iii. *Guest account*. An account that is neither for an employee nor a student of the College. This includes consultants, external members to College workgroups and committees, visitors to events, etc.
iv. *Privileged account*. An account with access to sensitive data, such as for finance managers, internal super users, system administrators, Web editors, IT outsourcing partners, etc.
v. *System administrator*. A privileged account used to deploy, configure or manage systems, such as a sysadmin, a database administrator, etc.
vi. *Application developer*. A user who develops an application with a programming language such as PHP, that others will use, directly or indirectly.
vii. *Super user*. A user that can change their identity, e.g. an employee who can login to a system as if they were another user, without using that user's credentials.

3. Accounts Creation

Guest accounts have an expiry date of one year or the activity completion date, whichever occurs first.

Generic accounts need to be authorised by the Director of Information Systems and Technologies; shall only be granted when there are no other alternatives. In particular they are not a suitable solution merely to share files or email, or in most service over the counter situations.

Privileged accounts need to be authorised by the Director of Information Systems and Technologies. In addition privileged accounts with access to sensitive data must be authorised by the Director or Delegate responsible for the information.

4. Requirements for System Administrators

Systems shall be configured to require authentication for login, even mobile devices (where a PIN or fingerprint may be appropriate). Exceptions shall be granted for specialized devices such as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only).

System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate brute force password attacks, such as locking an account for a few minutes after several failed login attempts.

Practicable measures shall be put in place to log successful and failed login attempts.

System administrators shall not use default passwords for administrative accounts.

System administrators shall reset passwords for user accounts or require users to reset their own passwords in situations where they became aware of a security risk related to the account.

5. Requirements for Application Developers

Application developers shall, whenever possible, develop applications that require secure protocols for authentication and communication.

Applications that implement authentication must allow roles or delegation of duties, thus giving the ability for an employee to take over the functions of another without having to know their password.

Whenever possible, in-house systems that are available outside the College network should re-use the portal's authentication through token passing. If passwords are required, they will not be stored in clear text or in any easily reversible form.

6. Requirements for Privileged Accounts

Privileged accounts cannot be generic, and their use must follow the principles of least required access, i.e. a privileged account cannot be used when a least privileged account will do.

The actions performed by these accounts are subject to additional daily monitoring.